CLAIMS

We claim:

1. A method for handling personally identifiable information, said method comprising:

providing in a computer a first set of object classes representing active entities in an information-handling process, wherein a limited number of privacy-related actions represent operations performed on data;

providing in said computer a second set of object classes representing data and rules in said information-handling process, wherein at least one object class has said rules associated with said data; and

handling transactions involving said personally identifiable information, using said computer and said object classes.

2. The method of claim 1, wherein said object classes include one or more object classes representing parties, selected from the group consisting of

a data user object class,

a data subject object class,

a guardian object class,

and a privacy authority object class.

3. The method of claim 1, wherein said object class, having said rules associated with said data, represents a filled paper form, including both collected data and rules regarding said collected data.

4. A method for improving the handling of personally identifiable information, said method comprising:

performing an initial assessment of an information-handling process;

constructing a model of said information-handling process, based on said initial assessment; and

providing output, based on said gathering and constructing, that identifies at least one way in which said personally identifiable information could be better handled;

wherein said constructing includes:

representing entities, data, and rules in said information-handling process by using a limited number of object classes;

representing operations performed on data by using a limited number of privacy-related actions; and

representing transactions by using said limited number of object classes and said limited number of privacy-related actions.

5. The method of claim 4, wherein said providing output further comprises identifying at least one way in which said information-handling process could be improved.

6. The method of claim 4, wherein said providing output further comprises identifying at least one way to improve compliance with a law or contract.

7. The method of claim 4, further comprising enforcing compliance with a law or contract.

8. The method of claim 4, further comprising designing a modification to said information-handling process, based on said constructing and providing.

9. The method of claim 8, wherein said designing a modification further comprises designing a modification to improve compliance with a law or contract governing said information-handling process.

10. The method of claim 4, wherein said limited number of object classes includes one or more object classes representing parties, selected from the group consisting of
a data user object class,
a data subject object class,
a guardian object class,
and a privacy authority object class.

11. The method of claim 4, wherein said limited number of object classes include at least one object class wherein rules are associated with data.

12. A system for handling personally identifiable information, said system comprising:
means for providing in a computer a first set of object classes representing active entities in an information-handling process, wherein a limited number of privacy-related actions represent operations performed on data;
means for providing in said computer a second set of object classes representing data and rules in said information-handling process, wherein at least one object class has said rules associated with said data; and
means for handling transactions involving said personally identifiable information, using said computer and said object classes.

13. The system of claim 12, wherein said object classes include one or more object classes selected from the group consisting of
a data user object class,
a data subject object class,
a guardian object class,
and a privacy authority object class.

14. The system of claim 12, wherein said object class, having said rules associated with said data, represents a filled paper form, including both collected data and rules regarding said collected data.

15. A computer-usable medium having computer-executable instructions for handling personally identifiable information, said computer-executable instructions comprising:
means for providing in a computer a first set of object classes representing active entities in an information-handling process, wherein a limited number of privacy-related actions represent operations performed on data;
means for providing in said computer a second set of object classes representing data and rules in said information-handling process, wherein at least one object class has said rules associated with said data; and
means for handling transactions involving said personally identifiable information, using said computer and said object classes.

16. The computer-usable medium of claim 15, wherein said object classes include one or more object classes representing parties, selected from the group consisting of

a data user object class,
a data subject object class,
a guardian object class,
and a privacy authority object class.

17. The computer-usable medium of claim 15, wherein said object class, having said rules associated with said data, represents a filled paper form, including both collected data and rules regarding said collected data.